E 4000-01-P

DEPARTMENT OF EDUCATION

[Docket No.: ED-2022-SCC-0147]

Agency Information Collection Activities; Submission to the Office of Management and Budget for Review and approval; Comment Request; NCES Data Security Requirements for Accessing Restricted Use Data

AGENCY: National Center for Education Statistics, Institute of Education Sciences, Department of Education.

ACTION: Notice.

SUMMARY: The National Center for Education Statistics (NCES) within the Institute of Education Sciences, U.S. Department of Education invites the general public and other federal agencies to comment on a proposed information collection. NCES plans to collect information from individuals to fulfill its data security requirements when providing access to restricted-use microdata for the purpose of evidence building. NCES's data security agreements and other paperwork along with the corresponding security protocols allow the agency to maintain careful controls on confidentiality and privacy, as required by law. NCES published this proposal for 60 days of public comment beginning November 25, 2022. The purpose of this notice is to allow for an additional 30 days of public comment on the proposed data security information collection, prior to submission of the information collection request (ICR) to the Office of Management and Budget (OMB).

DATES: Written comments on this notice must be received by [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER] to be assured of consideration. Comments received after that date will be considered to the extent practicable. Send comments to the address below.

ADDRESSES: Written comments and recommendations for proposed information collection requests should be submitted within 30 days of publication of this notice. Click on this link

www.reginfo.gov/public/do/PRAMain to access the site. Find this information collection request (ICR) by selecting "Department of Education" under "Currently Under Review," then check the "Only Show ICR for Public Comment" checkbox. Reginfo.gov provides two links to view documents related to this information collection request. Information collection forms and instructions may be found by clicking on the "View Information Collection (IC) List" link. Supporting statements and other supporting documentation may be found by clicking on the "View Supporting Statement and Other Documents" link.

FOR FURTHER INFORMATION CONTACT: For specific questions related to information activities, please contact Carrie Clarady, 202–245–6347 or carrie.clarady@ed.gov.

SUPPLEMENTARY INFORMATION: The Foundations for Evidence-Based Policymaking Act of 2018 mandates that the Office of Management and Budget (OMB) establish a Standard Application Process (SAP) for requesting access to certain confidential data assets. While the adoption of the SAP is required for statistical agencies and units designated under the Confidential Information Protection and Statistical Efficiency Act of 2018, it is recognized that other agencies and organizational units within the Executive branch may benefit from the adoption of the SAP to accept applications for access to confidential data assets. The SAP is to be a process through which agencies, the Congressional Budget Office, State, local, and Tribal governments, researchers, and other individuals, as appropriate, may apply to access confidential data assets held by a federal statistical agency or unit for the purposes of developing evidence. With the Interagency Council on Statistical Policy (ICSP) as advisors, the entities upon whom this requirement is levied are working with the SAP Project Management Office (PMO) and with OMB to implement the SAP. The SAP Portal is to be a single web-based common application for requesting access to confidential data assets from federal statistical agencies and units. The National Center for Science and Engineering Statistics (NCSES) within the National Science Foundation submitted a Federal Register Notice in September 2022 announcing plans to collect

information through the SAP Portal (87 FR 53793). OMB approved the SAP Portal for data collection in December 2022.

Once an application for confidential data is approved through the SAP Portal, NCES will collect information to meet its data security requirements. This collection will occur outside of the SAP Portal.

Title of the Collection: NCES Data Security Requirements for Accessing Restricted Use Data

OMB Control Number: 1850-NEW

Type of Review: New ICR

Respondents / Affected Public: State, Local and Tribal Governments

Total Estimated Number of Annual Responses: 80

Total Estimated Number of Annual Burden Hours: 60

Abstract:

Title III of the Foundations for Evidence-Based Policymaking Act of 2018 (hereafter referred to as the Evidence Act) mandates that OMB establish a Standard Application Process (SAP) for requesting access to certain confidential data assets. Specifically, the Evidence Act requires OMB to establish a common application process through which agencies, the Congressional Budget Office, State, local, and Tribal governments, researchers, and other individuals, as appropriate, may apply for access to confidential data assets collected, accessed, or acquired by a statistical agency or unit. This new process will be implemented while maintaining stringent controls to protect confidentiality and privacy, as required by law.

Data collected, accessed, or acquired by statistical agencies and units is vital for developing evidence on conditions, characteristics, and behaviors of the public and on the operations and outcomes of public programs and policies. This evidence can benefit the stakeholders in the programs, the broader public, as well as policymakers and program managers at the local, State,

Tribal, and National levels. The many benefits of access to data for evidence building notwithstanding, NCES is required by law to maintain careful controls that allow it to minimize disclosure risk while protecting confidentiality and privacy. The fulfillment of NCES's data security requirements places a degree of burden on individuals, which is outlined below.

The SAP Portal is a web-based application for requesting access to confidential data assets from federal statistical agencies and units. The objective of the SAP Portal is to broaden access to confidential data for the purposes of evidence building and reduce the burden of applying for confidential data. Once an individual's application in the SAP Portal has received a positive determination, the data-owning agency(ies) or unit(s) will begin the process of collecting information to fulfill their data security requirements.

The paragraphs below outline the SAP Policy, the steps to complete an application through the SAP Portal, and the process NCES uses to collect information fulfilling its data security requirements.

The SAP Policy

At the recommendation of the ICSP, the SAP Policy establishes the SAP to be implemented by statistical agencies and units and incorporates directives from the Evidence Act. The policy is intended to provide guidance as to the application and review processes using the SAP Portal, setting forth clear standards that enable statistical agencies and units to implement a common application form and a uniform review process.

The SAP Portal

The SAP Portal is an application interface connecting applicants seeking data with a catalog of data assets owned by the federal statistical agencies and units. The SAP Portal is not a new data repository or warehouse; confidential data assets will continue to be stored in secure data access facilities owned and hosted by the federal statistical agencies and units. The Portal will provide a

streamlined application process across agencies, reducing redundancies in the application process. This single SAP Portal will improve the process for applicants, tracking and communicating the application process throughout its lifecycle. This reduces redundancies and burden on applicants who request access to data from multiple agencies. The SAP Portal will automate key tasks to save resources and time and will bring agencies into compliance with the Evidence Act statutory requirements.

Data Discovery

Individuals begin the process of accessing restricted-use data by discovering confidential data assets through the SAP data catalog, maintained by federal statistical agencies at https://www.researchdatagov.org/. Potential applicants can search by agency, topic, or keyword to identify data of interest or relevance. Once they have identified data of interest, applicants can view metadata outlining the title, description or abstract, scope and coverage, and detailed methodology related to a specific data asset to determine its relevance to their research.

While statistical agencies and units shall endeavor to include metadata in the SAP data catalog on all confidential data assets for which they accept applications, it may not be feasible to include metadata for some data assets (e.g., potential curated versions of administrative data). A statistical agency or unit may still accept an application through the SAP Portal even if the requested data asset is not listed in the SAP data catalog.

SAP Application Process

Individuals who have identified and wish to access confidential data assets are able to apply for access through the SAP Portal. Applicants must create an account and follow all steps to complete the application. Applicants begin by entering their personal, contact, and institutional information, as well as the personal, contact, and institutional information of all individuals on their research team. Applicants proceed to provide summary information about their proposed

project, to include project title, duration, funding, timeline, and other details including the data asset(s) they are requesting and any proposed linkages to data not listed in the SAP data catalog, including non-federal data sources. Applicants then proceed to enter detailed information regarding their proposed project, including a project abstract, research question(s), literature review, project scope, research methodology, project products, and anticipated output. Applicants must demonstrate a need for confidential data, outlining why their research question cannot be answered using publicly available information.

Submission for Review

Upon submission of their application, applicants will receive a notification that their application has been received and is under review by the data owning agency or agencies (in the event where data assets are requested from multiple agencies). At this point, applicants will also be notified that application approval does not alone grant access to confidential data, and that, if approved, applicants must comply with the data-owning agency's security requirements outside of the SAP Portal, which may include a background check.

In accordance with the Evidence Act and the direction of the ICSP, agencies will approve or reject an application within a prompt timeframe. In some cases, agencies may determine that additional clarity, information, or modification is needed and request the applicant to "revise and resubmit" their application.

Data discovery, the SAP application process, and the submission for review are planned to take place within the web-based SAP Portal.

Access to Restricted-Use Data

In the event of a positive determination, the applicant will be notified that their proposal has been accepted. The positive or final adverse determination concludes the SAP Portal process. In the instance of a positive determination, the data-owning agency (or agencies) will contact the applicant to provide instructions on the agency's security requirements that must be completed to gain access to the confidential data. The completion and submission of the agency's security requirements will take place outside of the SAP Portal.

Collection of Information for Data Security Requirements

In the instance of a positive determination for an application requesting access to an IES/NCES-owned confidential data asset, NCES will contact the applicant(s) to initiate the process of collecting information to fulfill its data security requirements. This process allows NCES to place the applicant(s) in a trusted access category and includes the collection of the following information from applicant(s):

- Restricted-use licensing agreement – This document is an agreement between NCES and the applicant's organization stipulating that NCES's confidential data assets are provisioned exclusively for statistical purposes and that the applicant must handle and use the data in accordance with the terms and conditions stated in the agreement and all prevailing laws and regulations. The agreement requires signatures from the applicant(s) and a senior official at the applicant's organization who has the authority to enter the organization into a legal agreement with NCES. A Memorandum of Understanding is used in lieu of a restricted-use data licensing agreement for other government agencies.

- Security plan form – This document requests information from the applicant(s) to ensure the confidential data assets are protected from unauthorized access, disclosure, or modification. The information collected in the security plan form includes the following:

- planned work location address(es),
- workstation specifications (make, model, serial number, type, and operating system),
- workstation authorized users,
- workstation monitor position (to prevent unauthorized viewing), and
- workstation antivirus brand and version.

In addition, the applicant(s) must initial a series of security measures to indicate compliance. Finally, the form requires signatures from the applicant(s), a senior official at the applicant's organization, and a System Security Officer (SSO) at the applicant's organization. The SSO, in signing the Security plan form, assures the inspection and integrity of the applicant's security plan. A Security plan: Remote Access Only form is used in lieu of a Security plan form when the license is accessing data remotely.

- Affidavit of nondisclosure form – This document describes the confidentiality protections the applicant(s) must uphold and the penalties for unauthorized access or disclosure. The form requires signatures from the applicant(s) as well as the imprint of a notary public.
- Licensee training certificate – This document requests information from the applicant(s) to ensure the completion of the IES/NCES restricted-use data license training.

These documents and a more complete description of the NCES Data Security Process are available for public view during this 30D public comment period.

Estimate of Burden

The amount of time to complete the agreements and other paperwork that comprise NCES's security requirements will vary based on the confidential data assets requested. To obtain access to NCES confidential data assets, it is estimated that the average time to complete and submit

NCES's data security agreements and other paperwork and to complete the required training is 45 minutes. This estimate does not include the time needed to complete and submit an application within the SAP Portal. All efforts related to SAP Portal applications occur prior to and separate from NCES's effort to collect information related to data security requirements. The expected number of applications in the SAP Portal that receive a positive determination from NCES in a given year may vary. Overall, per year, NCES estimates it will collect data security information for 80 application submissions that received a positive determination within the SAP Portal. NCES estimates that the total burden for the collection of information for data security requirements over the course of the three-year OMB clearance will be about 180 hours and, as a result, an average annual burden of 60 hours.

Dated: May 4, 2023.

Stephanie Valentine,

PRA Coordinator,

Strategic Collections and Clearance,

Governance and Strategy Division,

Office of Chief Data Officer,

Office of Planning, Evaluation and Policy Development.

[FR Doc. 2023-09878 Filed: 5/9/2023 8:45 am; Publication Date: 5/10/2023]